Faces are Protected as Privacy

An Automatic Tagging Framework Against Unpermitted Photo Sharing in Social Media

Tang, Lihong; Ma, Wanlun; Grobler, Marthie; Meng, Weizhi; Wang, Yu; Wen, Sheng

Published in:
IEEE Access

Link to article, DOI:
10.1109/ACCESS.2019.2921029

Publication date:
2019

Document Version
Publisher's PDF, also known as Version of record

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON RECENT ADVANCES IN VIDEO CODING AND SECURITY

Received April 30, 2019, accepted May 21, 2019, date of publication June 5, 2019, date of current version June 21, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2921029

Faces are Protected as Privacy: An Automatic Tagging Framework Against Unpermitted Photo Sharing in Social Media

LIHONG TANG[1,2], WANLUN MA[3], MARTHIE GROBLER[4], WEIZHI MENG[5], YU WANG[1], AND SHENG WEN[2]

[1]School of Computer Science and Cyber Engineering, Guangzhou University, Guangzhou 510006, China
[2]School of Software and Electrical Engineering, Swinburne University of Technology, Melbourne, VIC 3122, Australia
[3]Department of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China
[4]Data61, CSIRO, Melbourne, VIC 3008, Australia
[5]Department of Applied Mathematics and Computer Science, Technical University of Denmark, 2800 Kongens Lyngby, Denmark

Corresponding author: Yu Wang (yuwang@gzhu.edu.cn)

This work was supported by the National Natural Science Foundation of China under Grant 61802080 and Grant 61802077.

ABSTRACT On social platforms like Facebook, it is popular and pleasurable to share photos among friends, but it also puts other participants in the same picture in jeopardy when the photos are released online without the permission from them. To solve this problem, recently, the researchers have designed some fine-grained access control mechanisms for photos shared on the social platform. The uploader will tag each participant in the photo, then they will receive internal messages and configure their own privacy control strategies. These methods protect their privacy in photos by blurring out the faces of participants. However, there is still some defect in these strategies due to the unpredictable tagging behaviors of the uploader. Malicious users can easily manipulate unauthorized tagging processes and then publish the photos, which the participants want them to be confidential in social media. To address this critical problem, we propose a participant-free tagging system for photos on social platforms. This system excludes potential adversaries through automatic tagging processes over two cascading stages: 1) an initialization stage will be applied to every new user to collect his/her own portrait samples for future internal searching and tagging, and; 2) the remaining unidentified participants will be tagged in cooperative tagging stage by the users who have been identified in the first stage. For the system evaluation of efficiency and effectiveness, we conducted a series of experiments. The results demonstrated the tagging efficiency (96% tagging rate and 0.77s/photo tagging speed on average), photo masking and unmasking efficiency (0.13s/face on average), and the privacy preserving performance (over 90% identities in both group and individual photo are preserved).

INDEX TERMS Social media, face tagging, privacy protection, system security.

I. INTRODUCTION

A. BACKGROUND

Social media have gradually changed people's default privacy settings by forming a ''sharing culture'' among online users. They start to tolerate, get used of, or even accept the exposure of their personal private information in social media platforms. For example, it was reported that 91% teenagers uploaded their own photos on Facebook (*i.e.* a famous social media platform), and 92% used to post their real name onto Facebook profile [1]. There are also online exhibitionism and narcissism (*i.e.* behaviors that are more open at sharing photos in social media), which have been regarded as actions of personal brand-building [2].

Along with the growing willingness to share, people are also reported to be less conscious of the content of photos they are going to upload. For example, there are 34% of Facebook users claimed that they did not think about the possible harm (*e.g.* leak of personal privacy) to their friends before they uploaded the photos [3]. In a survey recently run by Pew Research Centre (PRC) [4], they issued a questionnaire about why some users dislike using Facebook, and identified one of the most possible reasons as ''people can post someone's personal information (*e.g.* photos) without asking for

The associate editor coordinating the review of this manuscript and approving it for publication was Zhaoqing Pan.

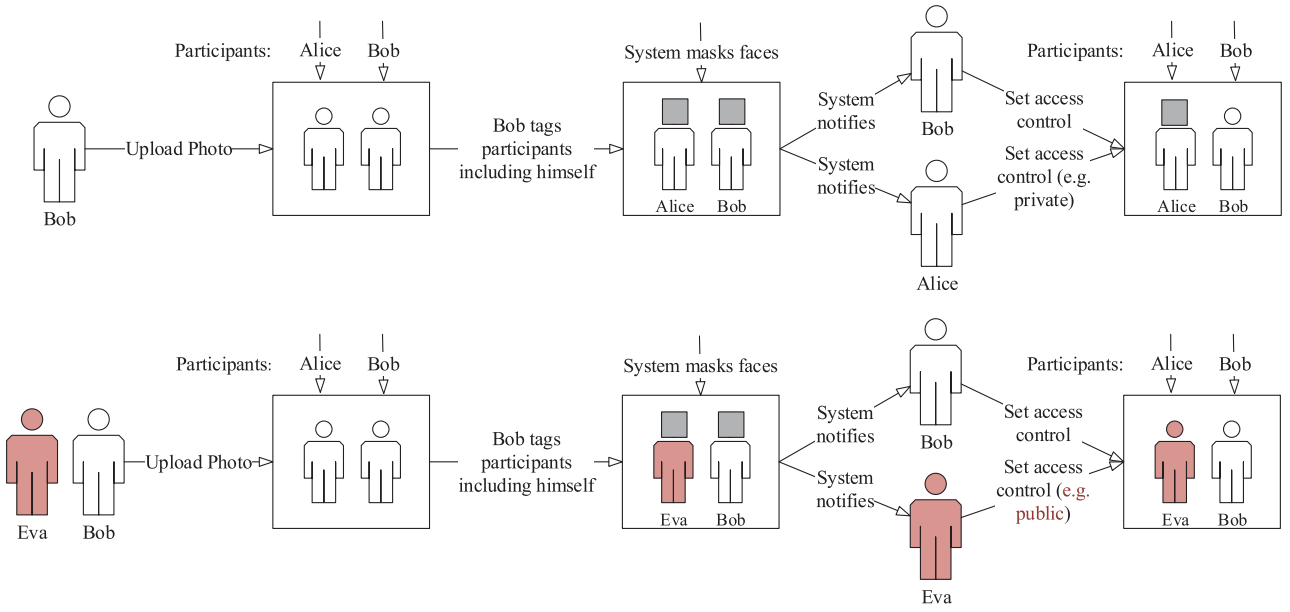

FIGURE 1. Malicious Tagging Behaviors: In the first scenario, Bob is an honest uploader and he will tag his friend Alice correctly in his uploaded photo. Once Alice receives the notification from Bob, she is able to set her own access control to determine who can view her own face in Bob's uploaded photo, the system will blur out Alice's face area if viewers do not get the permission given by Alice. In the second scenario, Bob works with Eva to set up Alice and tag Alice's face with Eva's name deliberately. In this case, once Eva confirms she is the face owner, she will have fully control over Alice's face. The face area which is supposed to be hidden could remain uncovered.

permissions''. In another survey posted by CNET [5], over 90% of photos that tagged users who were drunk or at other embarrassed moments will be untagged or even removed soon from their Facebook timeline, since the tagged users usually wanted them to be unseen from others.

These negative impacts are depressed but still under control, however sometimes, the harm is even worse and could be hard to estimate. For example, an inappropriate photo posted in social media may result in unemployment situation in some cases. It was reported that over 57% of small business employers are using social media to screen job candidates [6]. Among those employers, 45% of them have experiences of not hiring a candidate due to their provocative or inappropriate photographs collected from social networking sites. It is somewhat unfair to the unemployed candidates because these 'harmful' photos may not even be uploaded by the candidates themselves [7]. In another recent study run in Australia, 1 in 5 Australians were reported to be suffered from 'revenge porn', known as a spiteful sharing of sexually explicit portrayals via any media such as Facebook [8]. The situation was understandable when 11% of Australians claimed to have images shared online without their consents [9].

B. MOTIVATION

The above background suggested a situation of 'water and fire': 1) the nature of photo sharing in social media; 2) the potential harm to users' privacy caused by the photo sharing. In order to address the concerns on both sides, previous methods mainly adopted access control mechanisms onto social media photos from either photo-level [10]–[19] or face-level protection [20], [21]. In the photo-level category, only selective social media users were allowed to view the photos. However, a user who had the permission to view a photo could assess to all the information in the photo. Therefore, photo-level access control mechanisms were relatively coarse and they could hardly provide diverse privacy preserving protections if participants in a photo did have different requirements of sharing.

Distinguished from photo-level protection, The face-level protection provided a fine-grained solution by managing the access to each participant's face in the photo [20], [21]. Typically, each participant will be informed when the photo containing their faces are uploaded, and the participant will decide the access permission to his/her own face. For example, if a participant disallows the access to the photo containing his/her face in social media, his/her face will be blurred out by applying covers (*e.g.* mosaic). His/Her online friends who are not granted with access permissions will not see his/her appearance in the photo. This category of face-level access control mechanisms enabled personally privacy settings for each participants in photos and successfully handled the cases of interests conflicts of photo sharing in social media.

However, current face-level solutions were critically vulnerable to malicious tagging behaviors. Original face-level solutions heavily relied on reputations of photo uploaders [14]–[22]. If an adversary collude with a partner and deliberately tag victims' faces with the partner's name. The victims (*i.e.* face owners) could not be notified and lose the right of setting access control to their own faces. Fig. 1. illustrates the case of *malicious tagging attack*. In the first honest scenario, there are two participants in the

uploaded photo: Bob is the photo uploader and Alice is the photo co-owner. As an honest uploader, Bob tags Alice correctly in the photo. Once the system send the notification to Alice, she can set up her personal privacy policy to determine who has the permission to view her face in Bob's uploaded photo. For viewers who do not get Ailce's permission, they can only see the blur face of Alice. In the collusion scenario, Bob colludes with Eva to tag Alice as Eva intentionally. Once Eva confirms she is the face owner, she will get fully access control of Alice's face. In this case, Alice cannot set her own access control onto her own face. Therefore, a secure tagging mechanism takes a very critical part in face-level protection which should be seriously considered and designed.

C. OUR WORK AND CONTRIBUTIONS

To tackle the malicious tagging attack, this paper propose an automatic tagging framework against unpermitted photo sharing in social media. This novel framework applies face-level protection, but immunize to the malicious tagging attack. The core idea was to design a participant-free tagging mechanism, in which an individual's face could be automatically linked to a user's account. In this case, adversaries could not commit the malicious tagging attacks in the sharing of social media photos.

For the convenience of explanation and testing, we take Facebook as an example to illustrate and discuss our proposed framework. In fact, the proposed framework can be easily integrated into other social media platforms like Twitter, WeChat and other microblog services. We summarize our work and contributions as follow:

- We design a participant-free tagging framework to strengthen the robustness of existing face-level privacy protection in photo sharing. The proposed framework can avoid malicious tagging attacks.
- We carried out supporting research works (refer to Section IV-A & VII) to demonstrate the feasibility of the developed framework.
- We evaluated the performance of our developed framework in the context of Facebook. The results suggested that the newly develop framework is superior to all of the previous works.

The rest of the paper is organized as follows. We first elaborate the design of the system framework in Section 2. We show the ethics discussion in Section 3, and present system evaluation in Section 4. The related works is discussed in Section 5, and Section 6 discusses limitations and future work. We finally conclude this paper in Section 7.

II. ETHICS STATEMENT & DATA MANAGEMENT

Before we carried out our social survey, we submitted our full ethics application to Human Ethics Advisory Groups (HEAGs) in our faculty. In our application, we described our research, the types of people involved in our survey and the information we plan to gather. After we got the permission from the review board, we carried out our social survey and invited people to participant in. We have attached the questions of the social survey in Appendix. Readers could refer to Appendix for details.

Our research team asked people passing by in person if they would like to participant our survey. Before we asked them to complete the questionnaire [23], we gave them a copy of the Plain Language Statement and a sheet of printed questionnaire paper. Meanwhile, we simply explained the research purpose as well as the survey. No contact details of the participants will be collected during the conversation. Before they agreed to proceed, our research team made sure that people have understood the survey purpose, and we also made sure that they have read through the Plain Language Statement.

The survey relied on volunteers and their consents were implied by the return of survey questions. Any volunteers could return the results back to us either on-site or through emails later. Photo copies or scanned files were both acceptable. We do not reveal any information which could possibly link to their identity. We only accepted one submission per person. Considering volunteers' privacy, we renamed the files with random numbers if we thought the file name could possibly make them identifiable. When our research team received emails from volunteers, only the attachments were downloaded, and then we deleted the emails immediately to make the data unidentifiable. All surveys will be kept for at least 5 years after the publication, then destroyed. We explained to our volunteers that 1) withdrawal from this survey is not possible once the information has been de-identified, 2) their information will not be shared with or sold to anyone, and 3) volunteers are also welcome to contact the researchers for a summary of results.

III. SYSTEM DESIGN

Similar to previous work [21], we designed a web-based photo sharing application (*i.e.* Facebook App) that provided face-level privacy protection (*i.e.* participants' faces). The application was implemented and integrated into Facebook by leveraging platform's APIs. Distinguished from previous work, the new design has realized the automatic participant-free face tagging mechanism. In our system design, we reckon that only tagged users could set their own face access control (*i.e.* to decide who could view their own faces on a specific photo shared on Facebook). Only those who have been correctly tagged by our system could go for the cooperative tagging process.

The system framework is shown in Fig.2, which is composed of several stages. 1) the face identity initialization, 2) automatic face tagging process, 3) access control setting mechanism, and 4) photo rendering phase. Compared to previous works, our contributions are the face identity initialization and automatic face tagging process which are designed to mitigate the malicious tagging behaviors. In the above framework, we employed Facebook's APIs to retrieve users' face information so that the system can generate individual's face identity for later use. During the automatic face tagging

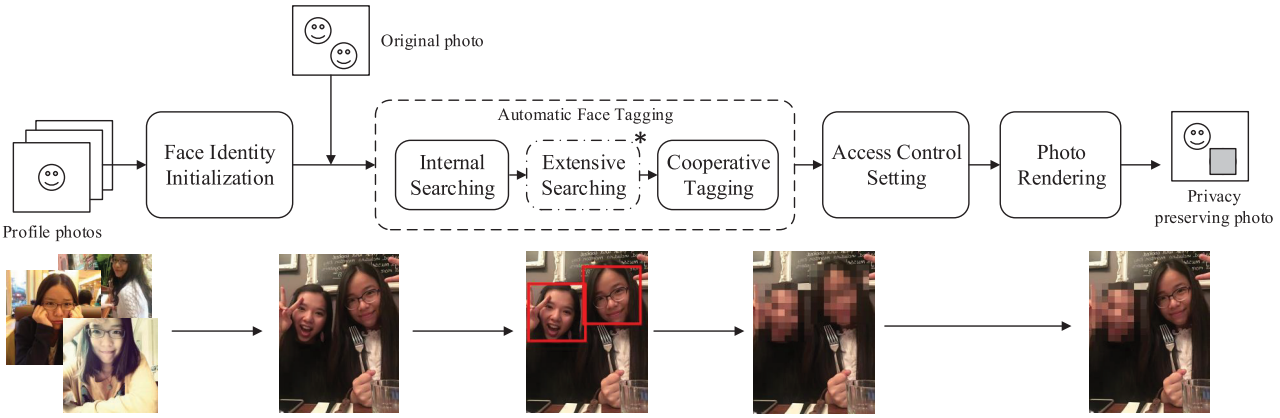

FIGURE 2. System Framework: Our system is composed of 1) the face identity initialization, 2) automatic face tagging process, 3) access control setting mechanism, and 4) photo rendering phase. Compared to previous works, our contributions are the face identity initialization and automatic face tagging process which are designed to mitigate the malicious tagging behaviors. In the above framework, we employed Facebook's APIs to retrieve users' face information so that the system can generate individual's face identity for later use. During the automatic face tagging process, we adopted face recognition technology developed by Microsoft for internal searching and cooperative tagging processes. The extensive searching is regarded as an option at the moment.

process, we adopted face recognition technology developed by Microsoft for internal searching and cooperative tagging processes. The extensive searching is regarded as an option at the moment and we will explain it in section VII.

A. SUPPORTING TECHNOLOGIES

1) API SUPPORT

There are two sets of APIs that can be used for our system design. These APIs are directly called by sending 'Ajax requests' to API providers' server.

The first set is provisioned by Facebook for the usage of users' information retrieval. Give an arbitrary user i on Facebook, we summarize the detailed tasks from the first set of APIs as follows: Once user i has authorized his/her Facebook account through our App, the system will retrieve user i's Facebook ID and a list of photos uploaded ($l_{ip} \in L_i, p \in N, p = 1, 2, 3 \ldots,$ n) by user i in Facebook.

The second set of APIs is provided by Microsoft Face as part of our auto-tagging process. Though Facebook has its own auto-tagging technique for face recognition, the performance highly relies on users' behaviors. Facebook users can either choose to untag or falsely tag faces. These behaviors potentially reduce the chance and accuracy of being automatically tagged in Facebook. Moreover, Facebook's internal face recognition does not support the usage of external Apps. Therefore, we redesigned the automatic tagging processes and utilized Microsoft Face to provide face recognition functions. This improved the performance of automatic tagging processes.

2) ACCESS CONTROL

Supporting technologies also include approaches about how the participants customize face-level access permissions to the photo containing their faces. Basically, online friends of a photo participant (*e.g.* user i) can only view the authorized area in the shared photo such as user i's face area after been authorized. If online friends' visit to the photo are not authorized by user i, the specific face area will be blurred out. In our work, the access control processes will be similar to the works [21]. In our system framework, we will reuse this part to implement the face-level protection. The access control module is located in the server side. For the implementation of the access control functions, readers could refer to previous works [21] for more details.

B. FACE IDENTITY INITIALIZATION

We decide to collect users' profile picture photos on Facebook to facilitate face recognition processes. The profile picture photos usually contain users' own faces. We have carried out an empirical survey in order to demonstrate this phenomenon (See details in section IV-A).

In the face identity initialization step (refer to Fig. 3), we define L_i to be the photo set of an arbitrary user i in Facebook. All the photos in user i's profile album will be collected and stored in L_i. Only when user i registers his/her Facebook account through our app for the first time, his/her photos will be collected and uploaded to set L_i. According to our empirical survey, the face set containing the largest number of faces is most likely to be user i's face set. Therefore, we first extract all the faces appearing in the photo set L_i, and then group them according to face similarity. The group that has the largest number of faces will be recognized as user i's face set F_i. The face areas in the set F_i are used as the primary training data of Facebook user i for the face recognition process. After training, we store user i's trained model (t_i) on the server side which will be used in auto-tagging process.

In our face identity generation, we designed 3 stages based on the survey results. 1) Collecting: first we will collect the faces depicted in users' Facebook profile picture album 2) Clustering: then our system will group faces according to the similarity by employing face recognition and comparison.

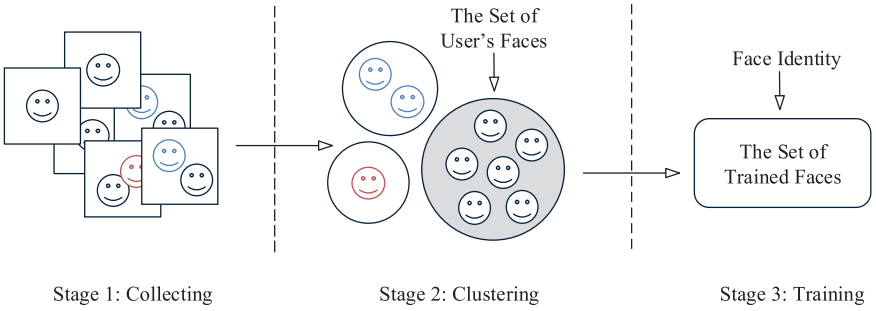

FIGURE 3. Generate Face Identity: In our face identity generation, we designed 3 stages based on the survey results. 1) Collecting: First we will collect the faces depicted in users' Facebook profile picture album 2) Clustering: Then our system will group faces according to the similarity by employing face recognition and comparison. The face set which has the largest number of faces is believed to the user's and 3) Training: Our system will then train the face set and generate the face identity.

The face set with the largest number of faces is considered to the user's and 3) Training: our system will then train the face set and generate the face identity.

C. AUTOMATIC FACE TAGGING

The second stage of the system framework is about automatic face tagging. The system will conduct face recognition on every face area once a photo is uploaded by Facebook users. If at least one face is recognized, the automatic tagging process will be activated. We proposed two different methods according to three consecutive sub-stages of performing automatic tagging processes: 1) Internal Searching: Face owner can be identified directly by our system, 2) Extensive Searching: Remaining untagged users could be identified by external public searching engine (*e.g.* Google), and 3) Cooperative Tagging: This sub-stage will be activated when there are still some participants who cannot be recognized by both internal and extensive searching sub-stages. In this section, we mainly focus on sub-stage 1 (internal searching) and sub-stage 3 (cooperative tagging). For sub-stage 2 (extensive searching), as its performance is mainly determined by the efficiency of third-party services, we will discuss it in Section VII for details.

1) INTERNAL FACE SEARCHING

We first introduce several variables to denote the factors that will be used to explain our proposed internal face searching sub-stage. Participants appearing in the uploaded photo v are gathered in set U_v and we specify an arbitrary participant in photo v as u_{vk} ($u_{vk} \in U_v$, $k = 1, 2, 3 \ldots, n$), so u_{vk} denotes the kth participant in the photo v. Then our system will compare the participant u_{vk} with every trained model t_i (i corresponds to the participant user i), which is pretrained and stored in our server side through the face identity initialization process. Then it returns a confidence score (p^i_{vk}) after each similarity comparison. The results, in terms of confidence scores, will suggest how likely the participant's face u_{vk} is related to user i. The confidence scores (p^i_{vk}) related to the participant u_{vk} will be gathered in the set P_{vk} for further determination. We finally choose a set of candidates (p^q_{vk}) of participant u_{vk} by judging whether p^i_{vk} exceeds the predefined threshold (ε) or not. Our system will then send an internal notification to the candidates and ask them to confirm whether they are the corresponding face owners respectively or not. Other participants' faces in the uploaded photo will stay unseen during the confirmation process. Note that, there will be only one true face owner. Other candidates are supposed to decline the ownership requests of the concerned face area. Once a candidate confirms the ownership of the face, his/her name will be tagged on the photo automatically. The access control on his/her face area will be set by the candidate.

In the above internal face searching sub-stage, if the system receives more than one confirmations from candidates related to only one face area, there must be some candidate/candidates who have made mistake/mistakes. This happens usually when different people look similarly to each other so that their confidence scores are higher than ε. According to our investigation, this mistake may be caused by malicious spoofing. Spoofing means that attackers adds portraits of others into the attackers' own profile photo album to deceive the face identification process. In some other scenarios, the mistake may be caused by the face areas from Twins. That is why, in our design, the internal searching will provide more than one candidates and our system will send face confirmation request to all the remaining candidates to avoid the false identification. If more than one candidate claim the ownership of a face area, our system will conduct the cooperative tagging process in which the real face owner are determined by the people who have been correctly tagged by the system. (refer to Section III-C2). We will also discuss some exceptional scenarios in Section III-D.

2) COOPERATIVE TAGGING

If there are still some remaining participants that our internal searching is unable to identify, the cooperative tagging process will be activated to help find the face owner. Note that cooperative tagging will only run when at least one face in the

Algorithm 1 Tagging Mechanism

Input: Detected faces (u_{vk}) in uploaded photo (v)
Output: Candidates of each depicted face in uploaded photo

```
for k ← 1 to n do
    for q ← 1 to m do
        confidence ← compareFaces(u_vk, t_q);
        if confidence ≥ ε then
            sendNotification(u_vk, t_q);
        end
    end
    if candidates.length() == 0 then
        cooperativeTaggingList ←
        putInCooperativeTaggingList(u_vk);
    end
end
```

photo have been correctly tagged in the previous sub-stages (refer to Section III-C1 & VII). Since the users who have been tagged are identified by our automatic tagging system, they are believe to be honest in cooperative tagging process. It is unlikely for them to falsely recognize the remaining participants in the photo because they apparently know who they were taking the photo with. Based on this intuition, our system allows these users who have been tagged are identified to tag the rest participants in a cooperative way. The cooperative tagging process will not be activated if only one person involves in this process, and the current tagging result will be regarded as the final result. If two or more participants involves in cooperative tagging process, our system will adopt the voting principle in this process to identify the face owner, which means that the candidate with the highest number of votes will be considered as the face owner. Additionally, there are some exceptional cases in the cooperative tagging sub-stages. For example, there is an exceptional that the only identified participant falsely tags the rest of depicted persons accidentally. In another case, someone may wrongly tag the remaining participant when two or more participants vote for the face owner. At this moment, different candidates may hold the same quantities of votes. The solutions to these exceptions will be handled in Section III-D.

D. EXCEPTION HANDLING

1) NO FACE HAS BEEN IDENTIFIED

The first exception is about 'no face has been identified'. With more details, no participant can be identified through all the previous sub-stages including internal searching, extensive searching, and cooperative tagging. According to our empirical studies (refer to Section IV-B1), this case rarely happens (around 96% successful tagging rate) but does exist particularly for those who never upload their photos online (comparatively 4%). In order to handle this exceptional case, our system permit the uploader to tag participants. The identified participants can view all other participants in the photo.However, this photo cannot be shared by anyone or appear in any other places but only uploader's homepage. The participants tagged by the uploader also cannot set their own access control.

2) FACE IS WRONGLY IDENTIFIED

The second exception is about 'face is wrongly identified'. With more details, the proposed system may wrongly identify a face or those authorized users may falsely tag a depicted participant in the cooperative tagging process (refer to Section III-C2). Once received the notifications from the system, each tagged participant will set their own access control after they have confirmed the face ownership. In the case, if the face sent to the tagged user is not his/hers, the user can response a negative confirmation to the notification, and the face will be blurred out if there is no user to claim the ownership of the face. Even though there may be some cases in which the tagging results of one depicted face are not consistent in cooperative tagging process, each face will go through the same confirmation process. Those faces are manually tagged by honest participants (*i.e.* the ones who have been certified by the system). We assume that the participants who are recognised by cooperative tagging process are honest and will not wrongly claim the faces which do not belong to them. Therefore, the privacy can be protected.

IV. SYSTEM VALIDATION

All the experiments below are conducted on an Amazon Web Server EC2 with 100MB/s down/up-link speed. On the server side, we adopted MySQL as our system database and the PHP version was 5.6.30. On the client side, we used MacBook Pro that has macOS Sierra system (version 10.12.6) installed. The test computer had memory of 16GB and the processor was 2.7 GHz Intel Core i7.

A. FEASIBILITY JUSTIFICATION

The core functions of the proposed system framework such as auto-tagging mechanism depends on users' uploaded photos that contain their own faces. To justify the feasibility of the proposed framework, we carried out an empirical survey to investigate how likely how likely social media users tend to use uploaded photos as their profile pictures. We mainly focused on Facebook users to run our experimental analysis. The results are shown in Fig. 4.

In the survey, we received 435 pieces of feedbacks. As shown in Fig. 4(A), 90.2% of Facebook users were using their own portraits as their profile pictures. This strongly supported the basis of the auto-tagging mechanism. In fact, a similar result can also be found in Knautz and Baran work [3]. The survey results also suggested that there were nearly 80% of Facebook users claim that the number of their own face areas that appeared in their own profile album was equal or larger than five. Moreover, as shown in Fig.4(B), 81% Facebook users claimed that more than half of the faces in their profile picture album belonged to themselves. This also supports the feasibility and effectiveness of the proposed

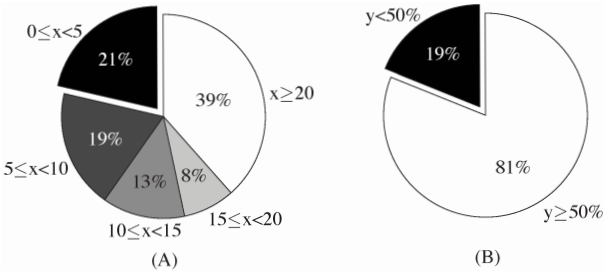

FIGURE 4. Survey Results. (A) The ratio of portraits that are used in Facebook users' profile album. It shows that nearly 80% users are using or once used their own portraits as the Facebook profile pictures. The number of their own faces found in their profile album is larger or equal to five. Only 21% users suggested that they uploaded the number of their own portraits less than five (as the black proportion shows). (B) Around 81% users claimed that the ratio of their own portraits was over 50% in the Facebook profile album.

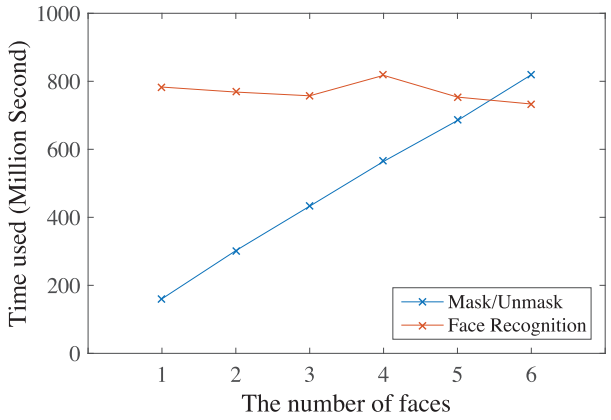

FIGURE 5. Efficiency Evaluation. 1) The red line denotes the time used for Face recognition process. The time consuming stay steady when the number of face areas that appear in a photo increases. The average time used is around 0.77s per photo. 2) The blue line denotes the time used for masking/unmasking process. The time increases linearly along with the number of faces appearing in a photo. In the second case, it costs around 0.13s to deal with a single face area averagely.

portrait auto-searching functions. Based on the survey results, we conclude that: 1) it is very likely that we can find face areas of Facebook users in their profile picture album, 2) users' own faces generally take the largest proportion among all the face areas that appear in their profile album. Therefore, we further optimize the searching functions by narrowing down the checking range from all the users' uploaded photos to the photos in their profile picture album only.

B. EFFICIENCY EVALUATION

In this subsection, we evaluate the efficiency of the auto-tagging mechanism and the photo masking process in terms of time consuming. The results are shown in Fig. 5.

1) TAGGING EFFICIENCY

The tagging efficiency highly depends on the accuracy and performance of the face recognition technology, the training data of face set, and the behavior of tagged users during the cooperative tagging process. The tagging efficiency is actually affected by three factors: 1) face recognition, 2) training data, and 3) tagging behaviors. The third factor (i.e. tagging behaviors) is highly related to personal characters, which cannot be easily examined through experiments. In fact, even though there may be some mistakes in the cooperative tagging process due to the unpredictable behavior of the tagged users, as long as they take part in this process, the tagging efficiency will be improved due to their honest confirmations. Therefore, in the following experiments, we will only investigate the influence caused by the face recognition and training data in terms of time consuming and tagging successful rate.

a: TIME CONSUMING

The time required for the tagging processes can be assessed by evaluating the time used for the face recognition processes. In the experiments, we organized six groups. Every group contains ten photos and the photos in same group have the same number of faces inside each photo. For example, every photo in group one only has one face inside, and every photo in group two will have two different faces inside. The same also happens in group three to group six. The results are shown in Fig. 5 (Red Line). We can see that the number of faces that appeared in a photo had little impact on the time consumed in the face recognition processes. We systematically investigated the reason for this phenomenon. We found that since our system use the face recognition service provided by Microsoft Face, the Internet condition has significant impact on the time used for this process. Therefore, when there was a good networking condition, the time consuming was steady. In our experiments, the average time for auto-tagging was around 0.77s per photo.

b: TAGGING SUCCESSFUL RATE

We also invited another 30 volunteers who have already used our system and generated their face identities in our server. We carried out an empirical study on the number of their portraits uploaded in their Facebook profile picture album. As shown in Fig. 6, all the volunteers have uploaded more than five photos that containing their portraits to the album. Each volunteer provides ten test photos containing their own faces (200 photos in total). We found out that our system achieved a high tagging successful rate (around 96% in Fig. 6) by using the Facebook profile pictures as the training data to generate the face identities.

2) MASKING/UNMASKING EFFICIENCY

We also evaluated the time used for masking or unmasking process. Intuitively, the time used in both grows with the increase of the number of faces in a photo, since blurring out the face areas takes the most time in these process. The results are shown in Fig. 5 (Blue line). We can see that with the number of faces areas in a photo growing, the time used for processing a masked or unmasked photo increased linearly. The increment was around 0.13s per face on average. Based on the experiment results, we concluded that the masking/unmasking efficiency did not fluctuate too much according to the experiment results.

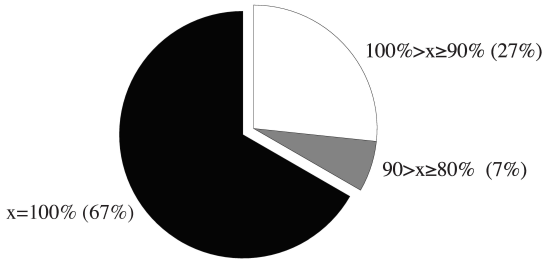

FIGURE 6. Tagging successful rate from 30 volunteers who have already generated their face identities in our server. The results showed that the tagging rate was around 96%. This proved that it was a solid solution to extract the face information from users' Facebook profile picture album to generate their face identities.

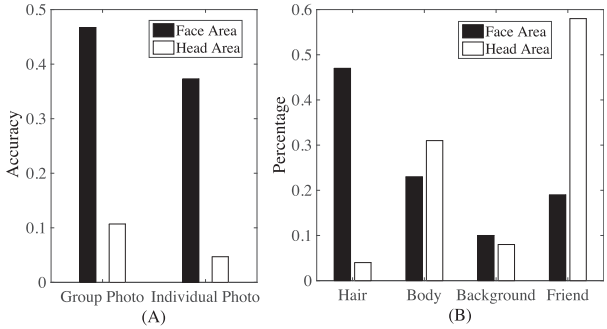

FIGURE 7. Privacy Preserving Result. The bar chart (A) illustrates the privacy preserving performance of our system. It shows that when only one face area is covered, 46.7% and 37.3% of users' identities are exposed in group photos and individual photos. As we enlarge the blur area from face area to head area, more than 90% of users' privacy is protected. In bar chart (B), it explains the reasons that why people can infer the right answer. When we only cover the face area, the main reason is the hair, and when we cover the entire head area, the main reason becomes the friend in the same photo.

C. PRIVACY EVALUATION

In this part, we will first evaluate the effect of the blur area's sizes on privacy protecting. Based on the result, we can then evaluate the effectiveness of our approach in preserving the privacy of depicted users. To do this, we invited 30 users to take part in our evaluation experiment. The number of the participants is the same as the previous work in [21].

1) IMPACT OF BLUR AREA'S SIZE ON PRIVACY PRESERVING

We invite 30 volunteers and show them some photos in which their friends depicted (the volunteers have not seen these tested photos before). There are totally 150 photos in the tested photo set, and we divide this set into 2 subsets in terms of the number of persons in the photos. The individual photo subset (N = 75) contains photos of only one person and the group photo subset (N = 75) contains photos of more than one persons. Additionally, for every photo in both subsets, we apply two different sizes of blur area: 1) face area (face rectangle directly obtained from API result) 2) head area (includes face and hair areas). The feedback from participants includes the content of the guessing on every masked user's name and the clues leading to their inference once they provide the right answer. The results are shown in Fig.7.

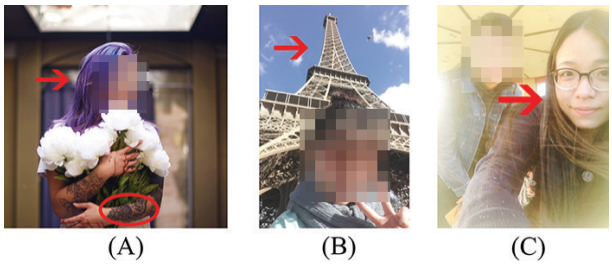

FIGURE 8. Privacy Evaluation Case. This figure shows the possible clues which could possibly lead to the right inferences. There are three reasons that we concluded from our experiments, they are hair, body features (A), background (B) and the friend in the same frame (C).

The results of our survey show that it is not enough to protect privacy if we only cover face area. 46.7% faces in group photos are correctly recognised while it is 37.3% in individual photos. The dominating clue for inferring the masked users correctly is the hair, and there are other helpful clues for correct inference, including user's body feature (*e.g.* figure, tattoo), photo background and the other friends appeared in one photo. The example images show in Fig. 8. As we enlarge the blur area with the multiplication of 1.85 from the original face rectangle, making sure all the user's face and hair area are covered and the other people in the same photo are less likely being influenced by the enlarged blur area. We find that over 90% of users' identities are preserved both in group photos and individual photos. The main reason why people can infer the right answer becomes the other friends in the same photo.

2) MALICIOUS TAGGING ATTACK MOCK-UP

In order to evaluate the robustness of privacy preserving of our system, we mock up several attacks by faking face identities and pretending to be other people. We register new Facebook accounts and upload A's portrait pictures in profile picture album of this newly registered account. A's portrait pictures are obtained from A's Facebook photo and A is also a member using our system. After we have uploaded a group photo containing A's face, our spoofing account did receive the confirmation notification. Even though we confirm the ownership of the faces through our spoofing account, we are still unable to apply our access control to A's face. Therefore, our system is immunized to the malicious tagging attack.

D. THRESHOLDS IMPROVEMENT

In order to improve the system efficiency, we randomly sample some faces from i's face set (F_i). These sampled faces are used as the user i's training data for the face recognition process. We assume that user i's album contains N photos. Each user returns an individual confidence score. These faces can be divided into two classes A and B according to the confidence scores. Class A contains faces providing higher confidence scores. The photos in Class A are the best training data for this user's face, and Class B contains the other users' faces with lower confidence scores. We also assume that n ($0 \leq n \leq N$) faces are selected at random from the user i's face set (F_i) without replacement. These faces are

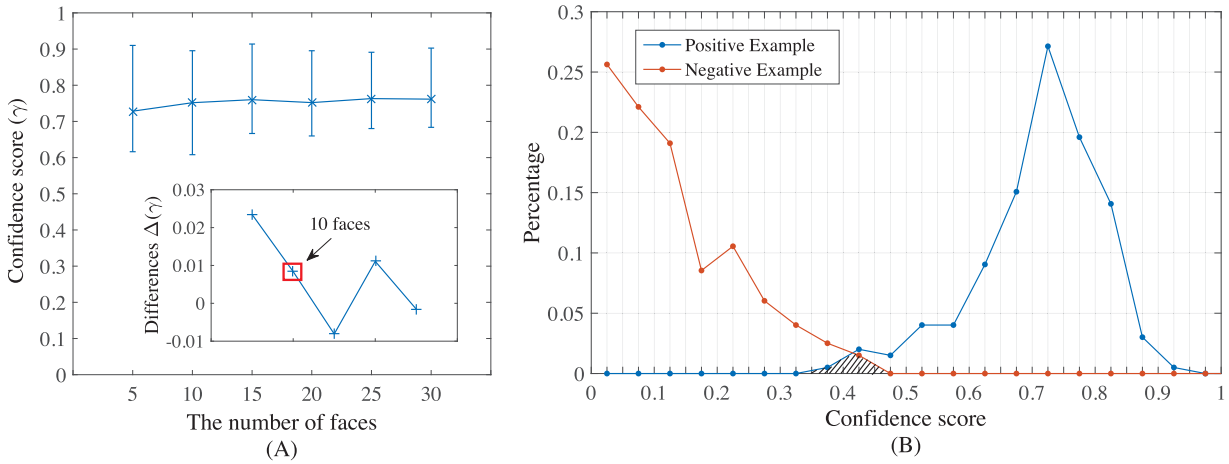

FIGURE 9. Experiment results on Thresholds. A) It explains how we determine the threshold NO.1, the largest number of faces used for each user to generate his/her face identity. The sub figure in Figure (A) shows the changes of differences of the confidence score $\Delta(\gamma)$ as we increase the number of faces used during the face identity initialization process. We set the threshold to be 10, because the line of the confidence score becomes more stable later on at the point where the face number is set to 10. B) It shows the distribution of the positive and negative examples of face recognition process, which is used for determining the threshold NO.2, the lowest confidence score that a face can be recognised as a certain person. In our design we adopted the number 0.46.

gathered in a subset ($subF_i$). Let X denote the number of faces belonging to Class A in $subF_i$. K denotes the number of faces in Class A. Moreover, N-K denotes the number of faces in Class B. We then use X as the hyper-geometric distribution with parameters K, N and n (i.e. X∼H(K, N, n)). We have the probability of $subF_i$ containing faces from Class A as

$$\begin{aligned} Pr(X \geq 1) &= 1 - Pr(X = 0) \\ &= 1 - f(x = 0|K, N, n) \\ &= 1 - \frac{\binom{N-K}{n}}{\binom{N}{n}}. \end{aligned}$$

We take one case from our experiments as an example. There are 200 faces in user i's face set (F_i). We assume that the faces with top 10% confidence scores belong to Class A. There are 20(200*0.1) faces in Class A and 180 faces in Class B. We randomly sampled 30 faces from F_i. Then, the probability of $subF_i$ containing faces from Class A is $Pr(X \geq 1) = 1 - Pr(X = 0) = 1 - \binom{200-20}{30} / \binom{200}{30} \approx 0.9676$. This result suggested that $subF_i$ containing at least one face with top 10% confidence score has a probability of 96.76%.

According to the work [24], if the sample size n represents a negligible fraction of the total population N, the hyper-geometric distribution with parameters K, N and n will be almost the same as the binomial distribution with parameters n and $p = K/N$, i.e. X∼B(n, p). Therefore, the probability of $subF_i$ containing faces from Class A when n is negligible compared to the total population N as

$$\begin{aligned} Pr(X \geq 1) &= 1 - Pr(X = 0) \\ &= 1 - f(x = 0|K, N, n) \\ &\approx 1 - f(x = 0|n, p) \\ &= 1 - \binom{n}{x} p^x (1-p)^{n-x} \\ &= 1 - (1-p)^n. \end{aligned}$$

In practice, if $N \geq 10n$, we use the binomial to approximate the hyper-geometric for very large values of N. Therefore, considering the above example, if there are more than 300 faces in user i's face set (F_i), the probability of $subF_i$ containing faces from class A is approximately $1 - (1 - 0.1)^{30} \approx 0.9576$, which is very close to the probability of hyper-geometric distribution, 96.67%.

We select 20 users and randomly sample some faces from their face sets. In our experiment, the sample size n are set to 5, 10, 15, 20, 25 and 30 respectively in each set. Fig. 9 illustrates the relationship between the confidence score of a specific sampled face set $subF_i^n$ (n as the sample size). The result shows that the confidence scores of the sampled face sets raise basically along with the increasing of sample size n. Meanwhile, the confidence score tends to be more smooth and stable as expected. Based on the above theoretical analysis and experiment result, we believe that the sample size of 10 is as good as enough, because it reaches a relatively high confidence score ($\gamma > 0.7$), meanwhile, the confidence score begins to become stable at this point. ($\Delta(\gamma) < 0.01$).

In addition to the size of face set to be trained, the predefined threshold of confidence score (ε) is also a significant parameter to determine whether the participant u_{vk} and the trained model t_i's owner i are the same person. If the predefined threshold is too large, *False Positives* (*FP*)(the fraction of different users that are falsely classified as identical) will be very small as expected, but *True Positives* (*TP*) (the fraction of identical users that are labelled as identical) will be small as well and vice versa. Therefore, the setting of the predefined thresholds is basically a trade-off between *True Positives* and *False Positives*.In order to protect privacy to the greatest extent possible, we set the threshold where *FP* rate is equal to zero according to zero tolerance principle. In our experiment, we have 201 positive case in which the depicted person is identical to the trained model owner while the

200 negative cases contains examples that the depicted person and the trained model owner is different. Fig. 9 shows the distributions of positive and negative cases in face recognition process. Therefore, we set the predefined threshold to be 0.46 where *FP* rate equals to zero.

V. RELATED WORK

Social media security issues have been largely studied in the last decade [25]–[30]. In the recent years, a lot of access control mechanisms have been developed to mitigate the risk of privacy leakage from photos uploaded on the social platform. According to the difference of their management of the access permission, these research work can be divided into two kinds: 1) coarse-grained: photo-level access control, 2) fine-grained: face-level access control. We will summery these two categorize of research work in the rest of this section.

A. PHOTO-LEVEL ACCESS CONTROL

The photo-level access control mechanisms is about applying access control on the photos to preserve users' privacy. In one hand, only selective social media users will be allowed to view the photo. On the other hand, a user who has the permission to view the photo can access to all the sensitive information inside the photo. Compared to the face-level access control mechanism, the photo-level one is relatively coarse-grained on the users' privacy preservation.

For example, Squicciarini *et al.* proposed a method to group previously uploaded photos and learned from users' access control preferences in each group to manipulate the access permissions for a newly uploaded photo [10]. Bounan *et al.* designed a security specification toolkit based on both security model and core ontology [11], [12], and they also used 'SWRL' language to address the security rules on the context of multimedia objects. In another work [13], Such and Rovatsos designed a mechanism to first measure the privacy and intimacy based on information theory, and then decide if personal information will be shared and whom it should be shared with. Among all the above works, the mechanisms in the first category could not provide individualized protection forms for each person in photos. They also could not invite the participants in photo to customize their own sensitive information.

Enabling multiparty collaborative tagging process for photos shared on social platform is another common approach to protect users' privacy, but it was still a photo level method. Xu *et al.* [14] designed a personal face recognition system for individuals in a co-photo and ask the co-owners to set their own privacy policy. Such *et al.* studied specific Multiparty Privacy Conflicts (MPCs) over co-owned photos [15]. Following a critical incident methodology, they conducted a survey to establish the empirical analysis about commonness, context and severity of privacy conflicts among photo co-owners. Besmer and Richter Lipford [16] designed a privacy management mechanism for uploaders and co-owners to negotiate whether the desired sharing photo should be released. However, the photo uploaders still have the highest priority and they could even ignore or reject the requests from tagged users. Hu et al. proposed a mechanism that involved multi-party to specify the access permission of each face in photos [17], [18]. the systematic approach will quantify the privacy risk and the desire of data sharing and then conduct a trade-off between privacy protection and photo sharing. Squicciarini *et al.* [19] presented a theoretical solution to the collective privacy management problem, which builds upon the well-known game theory — Clark Tax. However, this mechanism assumes that users can evaluate their individual preferences on sensitive information, which is unrealistic. Multiparty collaboration is considered the sharing interests of each participant in photos, but they did not specify how their approaches countered the cases in which there are non-tagged or wrongly tagged users. Additionally, the conflicts of sharing interests between uploaders and participants still exist.

B. FACE-LEVEL ACCESS CONTROL

In the category of face-level access control, privacy preserving mechanism is respectively employed for each participant in the photo. According to who has the privilege to customize diverse access permissions of participants in photo. In this subsection, the photo uploaders will tag each piece of sensitive information (*e.g.* faces of participants) to their 'owner'. Each participant will be invited to set their own access control. For example, Cutillo *et al.* [20] proposed an access control mechanism to protect a user's personally identifiable information (*i.e.* the face). Ilia *et al.* [21] proposed a preliminary solution dedicated to picture sharing, which takes advantage of inherent cooperation between users. Both of the solutions are fine-grained. In these works, every users associated with a photo are able to determine whether their faces can be viewed by others. When someone attempts to view a photo, the system presents the photo with the restricted faces blurred out if the face owners do not give the permission to the viewer. These works ([20], [21]) solved the cases of conflicting interests between the users. Besides, Yu *et al.* [31] proposed an approach based on deep multi-task learning, which can detect and recognize multiple classes of privacy-sensitive objects (i.e., faces of human beings) and provide recommended privacy settings for the image uploaders. However, all these methods highly depended on uploaders' behaviors. The sensitive information such as participants' faces, which were wrongly tagged by uploaders (*e.g.* malicious or careless users), could lead to fatal failures of the access control (refer to Section I-B for problem statement). Moreover, the mechanism proposed in [20] depended on a decentralized P2P-based online social networks, which was completely not applicable and scalable nowadays.

VI. LIMITATIONS

In this paper, we have implemented a framework to protect the privacy of social users in photo sharing. The experiments have

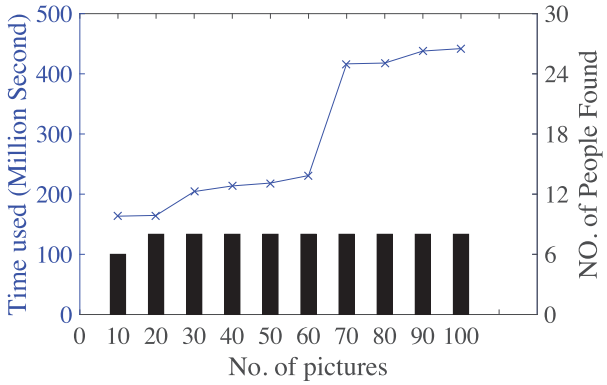

FIGURE 10. Time-consuming of External Searching. The curve shows that the average time for external searching process increases sharply at 60, because the maximum number of pictures shown out in the search results each time is 60, in another word, the average time for this process will increase sharply for each 60 pictures. The histogram explains that only 10% people's pictures can be acquired by extensive searching process, and the efficiency remains very low with the increase of pictures searched.

demonstrated the efficiency and effectiveness of the proposed auto-tagging method. However, there are still some issues that need more discussions and analysis.

A. EXTENSIVE SEARCHING

In the real world, some people do not like posting photos on their Facebook. In this case, we cannot get facial information from their Facebook profile. However, it is possible that these people who are actually the owners of the depicted faces cannot be found through our internal searching. According to the work [32], Facebook users tend to use real names into their Facebook network profiles. By taking this advantage, we can get their facial information through public searching engines (e.g. Google Image) since people are likely to post their own portraits on some other social network sites. We therefore design an extensive searching module in the framework.

We first test the efficiency of the extensive searching function. In the experiments, we collected names from ten people and searched them in Google Image to get their photos. The number of candidate photos we got from each round of searching ranged from ten to one hundred. As shown in Fig.10, the average time for this process increased sharply at sixty when more and more candidate photos were found. According to our analysis, the number 'sixty' came from the fact that the maximal number of images returned defaulted to sixty in each round of searching. It took more time when more candidate photos were collected, as shown in Fig.10. We second test the effectiveness of the extensive searching function. In the experiments, we collected eighty people from those who already have their face identities stored in our system. We also collected the top ten photos of each people from Google Image. We then compared their own photos with the ones collected from Google Image. As shown in Fig.10, only 10% people (*i.e.* 8 in 80) could succeeded in extensive searching. This experiment result demonstrated that only a few people's photos can be collected by searching in Google Image. In other words, the photos returned by the extensive searching module cannot provide useful face information about a specific person. There are something in common among the successful extensive searching people. For example, they are generally famous people who have social influence or have made outstanding achievements. In fact, it is hardly to retrieve the photos of most ordinary people in Google Image according to our studies. Due to the weak performance of the extensive searching module, we consider this part as an option in the whole framework. We will borrow some ideas from information retrieval field in the future to improve the efficiency of this part.

B. FACE RECOGNITION

The performance of face recognition techniques is a very critical to the success of our framework. According to our literature review [33], [34], current face recognition methods has achieved excellent performance on recognizing full face photos but not on profiles. We therefore tested the popular face recognition algorithms adopted in our framework. We found that most algorithms even did not recognize the profiles as a face object. As a result, the profiles were not successfully blurred out to preserve the privacy. Unfortunately, these profiles may be easily recognised by human beings through the hints of other factors in the photos (refer to Fig.6 and Section IV-C1). The solution to this limitation is strongly dependent on the development of the face recognition techniques, particularly the recognition performance on the profiles, which is out of the scope of our research in this paper. Currently, because most photos are with full faces or at least approximate full faces of participants, our current framework leave this limitation unsolved. We can easily extend and improve the framework by employing more robust face recognition algorithms in the future.

C. RELATIONSHIP LEARNING AND INTEGRATION

According to our evaluation experiments, people can figure out the ownership of a blurred portrait in photos even when the blurred areas are enlarged to make the 'guess' more challenging. However, as suggested in the experiment part (refer to Section IV-C1), this idea did not work well in protecting users' portraits. To address this problem, our opinion is to borrow ideas from social user profiling field [35], [36]. The idea is to study people's relationships based on their interaction on social networks. Access control mechanisms will be designed according to the strength of the pair-wise relationships. For example, C wants to view a photo having A and A's friend B in it, but A does not give C permission to view his face. Once system knows C is aware of the close friendship between A and B, the system will blur B's face as well no matter what access control has been set by B. However, in this case, sharing conflicts may arise in the framework. We leave this problem as an open issue for future studies.

VII. CONCLUSION AND FUTURE WORK

In this work, we proposed an automatic tagging framework to preserve users' privacy for photo sharing in social media.

The new framework could tackle the problem of malicious tagging from adversaries [20], [21]. To validate the newly developed framework, we carried out a number of supporting research works as well as experiments in the context of Facebook. In fact, the proposed framework can be easily integrated into other social media platforms like Twitter, WeChat and other microblog services. The experiment results indicated that our framework achieved the efficiency with 96% tagging rate.

There are also some future works based on the design presented in this paper. First, we will introduce new algorithms from information retrieval field to improve the performance of extensive searching module. This will make the framework more robust when social users seldom upload their portraits to social media platforms. Second, we may also apply new face recognition techniques to strength the accuracy of the framework. Last but not least, security certification, even some efforts on the propaganda of our framework, will be introduced to convince social media the safety of using our framework in terms of plugin to Facebook. As our framework highly depends on the adoption rate from users, more installation of the framework plugin in Facebook will guarantee the efficiency and effectiveness of the proposed work.

REFERENCES

[1] M. Madden, A. Lenhart, S. Cortesi, U. Gasser, M. Duggan, A. Smith, and M. Beaton, "Teens, social media, and privacy," Pew Res. Center's Internet & Amer. Life Project, Washington, DC, USA, Tech. Rep. 2013-Teens-Social-Media-And-Privacy, May 2013.

[2] L. Jaivin. *What Happened to Privacy?* Accessed: Jun. 8, 2019. [Online]. Available: https://www.abc.net.au/news/2016-10-24/linda-jaivin-privacy-and-its-discontents/7958882

[3] K. Knautz and K. S. Baran, *Facets of Facebook: Use and Users*. Hawthorne, NJ, USA: Walter de Gruyter, 2016.

[4] A. Smith. *What People Like and Dislike About Facebook*. Accessed: Jun. 8, 2019. [Online]. Available: https://www.pewresearch.org/fact-tank/2014/02/03/what-people-like-dislike-about-facebook/

[5] R. Trenholm. *Most Facebook Photos are Taken While We're Drunk, Survey Says*. Accessed: Jun. 8, 2019. [Online]. Available: https://www.cnet.com/news/most-facebook-photos-are-taken-while-were-drunk-survey-says/

[6] CareerBuilder. *Number of Employers Using Social Media to Screen Candidates has Increased 500 Percent Over the Last Decade*. Accessed: Jun. 8, 2019. [Online]. Available: https://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?sd=4%2f28%2f2016&id=pr945&ed=12%2f31%2f2016

[7] J. Bort. *A High School Coach was Fired for this Facebook Photo*. Accessed: Jun. 8, 2019. [Online]. Available: https://www.chron.com/technology/businessinsider/article/A-High-School-Coach-Was-Fired-For-This-Facebook-4975389.php

[8] J. Dent. *Revenge Porn: Image-Based Abuse Hits 'One in Five' Australians*. Accessed: Jun. 8, 2019. [Online]. Available: https://www.bbc.com/news/world-australia-39777192

[9] G. Kaszubska. *Not Just 'Revenge Porn'—Image-Based Abuse Hits 1 in 5 Australians*. Accessed: Jun. 8, 2019. [Online]. Available: https://www.rmit.edu.au/news/all-news/2017/may/not-just-_revenge-porn–image-based-abuse-hits-1-in-5-australian

[10] A. C. Squicciarini, S. Sundareswaran, D. Lin, and J. Wede, "A3P: Adaptive policy prediction for shared images over popular content sharing sites," in *Proc. 22Nd ACM Conf. Hypertext Hypermedia*, New York, NY, USA, 2011, pp. 261–270.

[11] B. A. Bouna, R. Chbeir, and A. Gabillon, "The image protector—A flexible security rule specification toolkit," in *Proc. Int. Conf. Secur. Cryptogr. (SECRYPT)*, Jul. 2011, pp. 345–350.

[12] B. A. Bouna, R. Chbeir, A. Gabillon, and P. Capolsini, "A flexible image-based access control model for social networks," in *Security and Privacy Preserving in Social Networks*. Vienna, Austria: Springer, 2013, pp. 337–364.

[13] J. M. Such and M. Rovatsos, "Privacy policy negotiation in social media," *ACM Trans. Auton. Adapt. Syst.*, vol. 11, no. 1, pp. 4:1–4:29, 2016.

[14] K. Xu, Y. Guo, L. Guo, Y. Fang, and X. Li, "My privacy my decision: Control of photo sharing on online social networks," *IEEE Trans. Dependable Secure Comput.*, vol. 14, no. 2, pp. 199–210, Apr. 2017.

[15] J. Such, J. Porter, S. Preibusch, and A. Joinson, "Photo privacy conflicts in social media: A large-scale empirical study," in *Proc. Conf. Hum. Factors Comput. Syst.*, 2017, pp. 3821–3832.

[16] A. Besmer and H. R. Lipford, "Moving beyond untagging: Photo privacy in a tagged world," in *Proc. SIGCHI Conf. Hum. Factors Comput. Syst.*, New York, NY, USA, 2010, pp. 1563–1572.

[17] H. Hu, G.-J. Ahn, and J. Jorgensen, "Detecting and resolving privacy conflicts for collaborative data sharing in online social networks," in *Proc. 27th Annu. Comput. Secur. Appl. Conf. (ACSAC)*, 2011, pp. 103–112.

[18] H. Hu, G.-J. Ahn, and J. Jorgensen, "Enabling collaborative data sharing in Google+," in *Proc. IEEE Global Commun. Conf. (ACSAC)*, Dec. 2012, pp. 103–112.

[19] A. C. Squicciarini, M. Shehab, and F. Paci, "Collective privacy management in social networks," in *Proc. 18th Int. Conf. World Wide Web*, 2009, pp. 521–530

[20] L. A. Cutillo, R. Molva, and M. Önen, "Privacy preserving picture sharing: Enforcing usage control in distributed on-line social networks," in *Proc. 5th Workshop Social Netw. Syst.*, 2012, pp. 6:1–6:6.

[21] P. Ilia, I. Polakis, E. Athanasopoulos, F. Maggi, and S. Ioannidis, "Face/off: Preventing privacy leakage from photos in social networks," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur.*, 2015, pp. 781–792.

[22] L. Tang, W. Ma, S. Wen, M. Grobler, Y. Xiang, and W. Zhou, "My face is mine: Fighting unpermitted tagging on personal/group photos in social media," in *Proc. Int. Conf. WISE*. Cham, Switzerland: Springer, 2017, pp. 1–12.

[23] *Facebook Image Privacy*. Accessed: Jun. 8, 2019. [Online]. Available: https://www.wjx.cn/jq/17992661.aspx

[24] M. H. DeGroot and M. J. Schervish, "Special distribution," in *Probability and Statistics*, 4th ed. London, U.K.: Pearson, 2012. [Online]. Available: http://www.mypearsonstore.com/bookstore/probability-and-statistics-9780321500465

[25] T. Wu, S. Wen, S. Liu, J. Zhang, Y. Xiang, M. Alrubaian, and M. M. Hassan, "Detecting spamming activities in twitter based on deep-learning technique," *Concurrency Comput., Pract. Exper.*, vol. 29, no. 19, 2017, Art. no. e4209.

[26] S. Wen, M. Sayad Haghighi, C. Chen, Y. Xiang, W. Zhou, and W. Jia, "A sword with two edges: Propagation studies on both positive and negative information in online social networks," *IEEE Trans. Comput.*, vol. 64, no. 3, pp. 640–653, Mar. 2015.

[27] J. Jiang, S. Wen, S. Yu, Y. Xiang, and W. Zhou, "Identifying propagation sources in networks: State-of-the-art and comparative studies," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 465–481, 1st Quart., 2017.

[28] E. Luo, Q. Liu, and G. Wang, "Hierarchical multi-authority and attribute-based encryption friend discovery scheme in mobile social networks," *IEEE Commun. Lett.*, vol. 20, no. 9, pp. 1772–1775, Sep. 2016.

[29] S. Chen, G. Wang, G. Yan, and D. Xie, "Multi-dimensional fuzzy trust evaluation for mobile social networks based on dynamic community structures," *Concurrency Comput., Pract. Exper.*, vol. 29, no. 7, p. e3901, 2017. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/cpe.3901

[30] C.-Z. Gao, Q. Cheng, X. Li, and S.-B. Xia, "Cloud-assisted privacy-preserving profile-matching scheme under multiple keys in mobile social network," *Cluster Comput.*, Feb. 2018. doi: 10.1007/s10586-017-1649-y.

[31] J. Yu, B. Zhang, Z. Kuang, D. Lin, and J. Fan, "iPrivacy: Image privacy protection by identifying sensitive objects via deep multi-task learning," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 5, pp. 1005–1016, May 2017.

[32] R. Zafarani and H. Liu, "Connecting users across social media sites: A behavioral-modeling approach," in *Proc. 19th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, New York, NY, USA, 2013, pp. 41–49.

[33] W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld, "Face recognition: A literature survey," *ACM Comput. Surv.*, vol. 35, no. 4, pp. 399–458, 2003.

[34] A. F. Abate, M. Nappi, D. Riccio, and G. Sabatino, "2D and 3D face recognition: A survey," *Pattern Recognit. Lett.*, vol. 28, no. 14, pp. 1885–1906, 2007.

[35] C.-C. Hung, Y.-C. Huang, J. Y.-J. Hsu, and D. K.-C. Wu, "Tag-based user profiling for social media recommendation," in *Proc. Workshop Intell. Techn. Web Personalization Recommender Syst. (AAAI)*, 2008, pp. 49–55.

[36] R. Li, S. Wang, H. Deng, R. Wang, and K. C.-C. Chang, "Towards social user profiling: Unified and discriminative influence model for inferring home locations," in *Proc. 18th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, 2012, pp. 1023–1031.